Exhibit R-2, RDT&E Budget Item Justification: PB 2015 Army											Date: March 2014	
Appropriation/Budget Activity 2040: *Research, Development, Test & Evaluation, Army* / BA 7: *Operational Systems Development*					R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*							
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
Total Program Element	-	14.314	9.351	14.175	-	14.175	19.054	19.318	20.811	19.057	Continuing	Continuing
491: *Information Assurance Development*	-	7.547	5.110	7.201	-	7.201	9.619	9.912	10.795	8.809	Continuing	Continuing
501: *Army Key Mgt System*	-	6.767	1.305	1.184	-	1.184	2.303	2.154	2.466	-	-	16.179
DV4: *Key Management Infrastructure (KMI)*	-	-	1.501	2.164	-	2.164	2.364	2.169	2.072	3.333	Continuing	Continuing
DV5: *Crypto Modernization (Crypto Mod)*	-	-	1.435	3.626	-	3.626	4.768	5.083	5.478	6.915	Continuing	Continuing

The FY 2015 OCO Request will be submitted at a later date.

Note

In FY15 the following adjustments were made:

Adjustment 1: DV4 Key Management Infrastructure was decreased $.489 Million while DV5 Crypto Modernization was increased $.852 Million, for a net increase of $0.363 Million.

Adjustment 2: Army Key MGT System funding was reduced by $1.227 Million.

Adjustment 3: Information Assurance funding was reduced by $2.443 Million.

A. Mission Description and Budget Item Justification

Information Asurance Development supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies into the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms into specific systems in support of securing the National Network Enterprise. This entails architecture studies, system integration, testing, certification, and accreditation of COMSEC systems and equipment. COMSEC technology ensures total signal and data security for all Army information systems to include any operational enhancement and specialized Army configurations. The program also assesses, develops, and integrates COMSEC tools (hardware and software) which provide protection for fixed infrastructure posts, camp or station networks as well as tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization Strategy.

Information Assurance Development funding supports the technical assessment and specifications documentation of cryptographic, key management and Information Assurance (IA) technologies developed under the direction of the National Security Agency (NSA), the Defense Information Systems Agency (DISA), Joint Services,

and commercial developers to secure National Security Systems (NSS) and National Security Information (NSI). Technical evaluations assess the security, operational effectiveness and network interoperability of advanced concept technologies to identify fundamental building blocks for Army IA solutions.

The Army Key Management System (AKMS) is the Army's implementation of the National Security Agency's (NSA) Electronic Key Management System (EKMS) program automating the functions of Communications Security (COMSEC) key management, control, and distribution, thereby limiting adversarial access to, and reducing the vulnerability of, Army Command, Control, Communications, Computers, Intelligence (C4I) systems. NSA's legacy EKMS infrastructure began its transition to the Key Management Infrastructure (KMI) in FY2012. The transition is set to be completed by the EKMS sunset date of December 2017 and will require a minimum of 528 Management Client Nodes (MGCs) to transition the existing Army COMSEC accounts from Local COMSEC Management System (LCMS) to KMI.

Key Management Infrastructure (KMI) provides an integrated, operational environment that will bring essential key management personnel and functions in-band. KMI achieves an over the network key (OTNK) management solution to support emerging cryptographically modernized systems. The KMI client nodes are the Army's subset of the National Security Agency's (NSA's) KMI Program supporting DoD Global Information Grid (GIG) Net Centric and Crypto Modernization Initiatives and supports emerging requirements transitioned from the Army Key Management System (AKMS). The Mission Planning/Mission Support System (MP/MSS) Interface for KMI will create a secure and highly automated interface to enable transparent provisioning of KMI products. The interface shall facilitate transparent communications between MP/MSS and KMI to achieve integration by bridging the gap between provisioning services and the communications net plan of the Warfighter.

The Crypto Modernization program supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies into the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms into specified systems in support of securing the National Network Enterprise in as transparent a manner as possible.

B. Program Change Summary ($ in Millions)	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total
Previous President's Budget	15.961	9.357	17.482	-	17.482
Current President's Budget	14.314	9.351	14.175	-	14.175
Total Adjustments	-1.647	-0.006	-3.307	-	-3.307
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Other Adjustments 1	-0.833	-0.003	0.363	-	0.363
• Other Adjustments 2	-0.814	-0.001	-1.227	-	-1.227
• Other Adjustments 3	-	-0.002	-2.443	-	-2.443

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
491: *Information Assurance Development*	-	7.547	5.110	7.201	-	7.201	9.619	9.912	10.795	8.809	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

Note

PE 0303140A, project 491 includes funding for the Army CIO/G6 and Project Director (PD) COMSEC.

A. Mission Description and Budget Item Justification

This program supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies into the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms into specified systems in support of securing the National Network Enterprise in as transparent a manner as possible.

This entails architecture studies, system integration and testing, installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates Information Assurance (IA)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp and station networks as well as efforts on tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan.

Funding supports the technical assessment and specifications documentation of cryptographic, key management and IA technologies developed under the direction of the NSA, the Defense Information Systems Agency (DISA), Joint Services, and commercial developers to secure National Security Systems (NSS) and National Security Information (NSI). Technical evaluations assess the security, operational effectiveness and network interoperability of advanced concept technologies to identify fundamental building blocks for Army IA solutions. (CIO/G6)

Develop and publish the strategy to identify and manage the insertion of new security capabilities to bridge operational gaps, providing timely security and performance improvements to the Army's network through the performance of interoperability and standards testing, conducting IA System of System Network Vulnerability Assessments IA SoS NVA) of Army Capability Sets, and develops and integrates IA/COMSEC capabilities to provide protections for fixed infrastructure post, camp and station networks. Develop Army migration strategies of COMSEC equipment to ensure fully IA-compliant solutions that meet the objective for LandWarNet (LWN) 2020 and beyond. (CIO/G6)

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Assessing emerging COMSEC hardware and software systems and products	0.835	-	0.112
Articles:	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Description: This program researches, assesses, tests and plans for cryptographic and information assurance technology insertions within the existing and future network infrastructure. It provides the basis for adjusting COMSEC capabilities and policies to reflect the latest technologies. Supports risk mitigation of IA networked vulnerabilities in end-to-end network operations and common operating environment. ***FY 2013 Accomplishments:*** This program researches new cryptographic, information assurance technologies, perform operational assessments, concept exploration and validation to develop strategies and policies capitalizing on and leveraging emerging cryptographic technologies. Continuing to provide information, knowledge sharing and new equipment capabilities, limitations, and impacts on the Army network to assist in bridging the gap between the tactical edge and the Army Enterprise Network. Test proof of concept devices and provide infrastructure support to facilitate information assurance technology transition. Continue to provide guidance for the adjustment of COMSEC programs and ensure COMSEC policies remains in synchronization with the latest COMSEC technologies. ***FY 2015 Plans:*** This program researches new cryptographic, information assurance technologies, perform operational assessments, concept exploration and validation to develop strategies and policies capitalizing on and leveraging emerging Cryptographic technologies. Continuing to provide information, knowledge sharing and new equipment capabilities, limitations, and impacts on the Army network to assist in bridging the gap between the tactical edge and the Army Enterprise Network. Test proof of concept devices and provide infrastructure support to facilitate information assurance technology transition. Continue to provide guidance for the adjustment of COMSEC programs and ensure COMSEC policies remains in synchronization with the latest COMSEC technologies.			
Title: Cryptographic Systems Test and Evaluation	2.205	1.914	-
Articles:	-	-	-
Description: This program supports the Army Cryptographic Modernization Transformational Initiative. This is accomplished by providing test and evaluation capabilities to the COMSEC community in order to assess emerging technologies before being released and approved for Army use; testing can be performed on hardware, software, or network systems. ***FY 2013 Accomplishments:*** The program will continue to test and evaluate advanced prototypes and cryptographic devices to confirm capability and interoperability on Army networks and systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. Continuing to evaluate performance of Cryptographic Modernization (CM) compliant devices, including the initial Suite B Internet Protocol Security (IPSec) devices built based on commercial standards. This is the first step in the migration to			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
NSA approved COTS devices for Secret and below information in place of Government Off-The-Shelf (GOTS) devices. Started evaluation of Secure Smartphones based on COTS platform for Mobile secure use. Evaluating KMI CI-2, Spiral 2 initial release and migration of initial HAIPE 4.0 compliant crypto devices to KMI based key delivery. Development plan for delivery of NSA produced keys for COTS devices. Complete evaluation of the performance of initial EKMS / AKMS to KMI transition strategies. These efforts will support network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating Information Assurance (IA) vulnerabilities to the national network enterprise. ***FY 2014 Plans:*** The program tests and evaluates systems to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program tests and evaluates Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. Develops interfaces and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluates performance of technologies and provide direction on were technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data.			
Title: Research and insertion of emerging Cryptographic and IA technologies, operational value, and performance improvement to shape policies and guidance (CIO/G6) ***Articles:*** ***Description:*** This program provides oversight and guidance for technical research and evaluation of Cryptographic and Key Management capabilities for IA compliance. This effort gained IT efficiencies and improved the performance on the Network by leveraging standardized COMSEC capabilities that are interoperable and supportable in Army, Joint and coalition networks/ systems. Army Collaborated and participated in Joint and Army Capability Technology Demonstrations to improve, define, develop and publish IA standards for new/modernized technology to support the LWN 2020 and Beyond. Assessed risk mitigation of IA network vulnerabilities in end-to-end Army network operations and Common Operating Environment. ***FY 2013 Accomplishments:*** This program researches new and emerging Cryptographic and IA technologies to bridge the operational gaps to enable secure communications between the tactical edge, the Army Enterprise Network and the DoD Joint Information Environment (JIE). Review operational needs, operation assessments, identify fundamental building blocks for IA solutions and risk reduction lab test commercial products for Army insertion. Participate in DOD pilot programs. Develop strategies and policies capitalizing on leveraging emerging cryptographic and key management technologies to enhance cyber security, prevent any undue risk and limitations and maximize performance to the Army networks. Effectively provide strategies, policies, and documentation to protect	4.507 -	3.196 -	7.089 -

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
information, and knowledge sharing on the LandWarNet to secure the edge. Provide guidance for the adjustment of COMSEC programs and ensure COMSEC policies remains in synchronization with the latest COMSEC technologies. (G6 OA22) ***FY 2014 Plans:*** This program researches new and emerging Cryptographic and IA technologies to bridge the operational gaps to enable secure communications between the tactical edge, the Army Enterprise Network and the DoD Joint Information Environment (JIE). Review operational needs, operation assessments, identify fundamental building blocks for IA solutions and risk reduction lab test commercial products for Army insertion. Participate in DOD pilot programs. Develop strategies and policies capitalizing on leveraging emerging cryptographic and key management technologies to enhance cyber security, prevent any undue risk and limitations and maximize performance to the Army networks. Effectively provide strategies, policies, and documentation to protect information, and knowledge sharing on the LandWarNet to secure the edge. Provide guidance for the adjustment of COMSEC programs and ensure COMSEC policies remains in synchronization with the latest COMSEC technologies. (G6 OA22) ***FY 2015 Plans:*** The COMSEC Modernization effort determines the maturity and viability of Cryptographic and Information Assurance (IA) technologies to ensure resolution of key interoperability issues prior to implementation while increasing operational availability and more rapid integration, document their operational value and provide a more secure network resulting in delivery of performance based standards consistent with the COE and the DoD Joint Information Environment (JIE). Review operational needs, operation assessments, identify fundamental building blocks for IA solutions and perform risk reduction lab tests of commercial products for Army insertion. Exercise oversight and evaluation aimed at improving process and technical solutions before making investment strategy decisions aimed at reducing or eliminating duplication. Participate in operational assessment and technology documentation of NSA, DoD, Joint Staff and Service led Joint Capability Technology Demonstrations (JCTD) aligned to documented Army and Service capability gaps for National Security Systems. Develop strategies and policies that leverage emerging cryptographic and key management tools and services. (CIO/G6)			
Accomplishments/Planned Programs Subtotals	7.547	5.110	7.201

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• DV5: *Cryptographic Systems RDTE*	-	1.435	3.626	-	3.626	4.768	5.083	5.478	6.915	Continuing	Continuing
• TA0600: *Information System Security Program - ISSP*	37.139	13.245	2.113	-	2.113	0.204	0.111	-	0.003	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• B96002: *Cryptographic Systems OPA2*	-	4.334	18.151	-	18.151	19.567	21.616	20.476	20.576	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	-	2.093	3.521	-	3.521	2.551	2.597	2.680	3.225	Continuing	Continuing

Remarks

0303140A DV5 - Cryptographic System - RDTE funds
TA0600 - Information System Security Program - OPA2 funds
B96002 - Cryptographic Systems - OPA2 funds
BS9716 - NON PEO-SPARES - OPA4 funds

D. Acquisition Strategy

The objective of this program is to integrate and validate hardware and software solutions that will secure current and objective architecture and electronic business/ commerce transactions. The objective of the Cryptographic Systems program is to provide adaptive, flexible, and programmable cryptographic systems using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic systems. The network operations effort will support the network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating Information Assurance (IA) networked vulnerabilities to National information security systems.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	C/CPFF	CECOM RDEC : CECOM RDEC APG, MD	73.320	0.821		0.842		0.112		-		0.112	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/FFP	DSCI Consulting : APG, MD	6.396	0.485		0.225		-		-		-	-	7.106	-
Engineering Support	C/CPFF	CACI : APG, MD	3.600	0.915		0.503		-		-		-	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	Booz Allen Hamilton : APG, MD	2.730	0.334		0.344		-		-		-	-	3.408	-
Engineering Support	C/FP	CSC : APG, MD	16.448	-		-		-		-		-	-	16.448	-
Engineering Support (G6/ OA22)	C/FP	CACI : APG, MD	0.000	1.513		1.219		2.647	Mar 2014	-		2.647	Continuing	Continuing	Continuing
System Engineering (G6/ OA22)	SS/LH	CECOM RDEC : APG, MD	0.000	-		-		1.673		-		1.673	Continuing	Continuing	Continuing
Engineering Support (G6/ OA22)	C/CPFF	Booz Allen Hamilton : APG, MD	0.000	1.530		1.277		0.951	Mar 2014	-		0.951	Continuing	Continuing	Continuing
Engineering Support (G6/ OA22)	C/FFP	AASKI : Edgewood, MD	0.000	-		-		0.632		-		0.632	Continuing	Continuing	Continuing
Service (G6/OA22)	SS/LH	ARL/SLAD : White Sand Missile Range (WSMR)	0.000	1.464		0.700		1.186		-		1.186	Continuing	Continuing	Continuing
Hardware/Software Engineering	C/FFP	CECOM RDEC : APG, MD	5.224	-		-		-		-		-	Continuing	Continuing	Continuing
Information Assurance System Engineering Support	C/FFP	MITRE : McLean, VA	3.328	-		-		-		-		-	-	3.328	-
C2 Protect Common Tools	C/FFP	CECOM RDEC : APG, MD	9.899	-		-		-		-		-	-	9.899	-
Engineering Support	C/FFP	VIATECH : APG, MD	8.119	0.485		-		-		-		-	-	8.604	-
Mission Planning Mission Support System (MPMSS) Interface	C/IDIQ	NSA (SAIC) : San Diego, CA	4.500	-		-		-		-		-	-	4.500	-

Exhibit R-3, RDT&E Project Cost Analysis: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 491 / *Information Assurance Development*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Network Operations	C/IDIQ	TBD : TBD	1.941	-		-		-		-		-	-	1.941	-
		Subtotal	135.505	7.547		5.110		7.201		-		7.201	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Test Support	C/CPFF	TBD : TBD	1.598	-		-		-		-		-	-	1.598	-
		Subtotal	1.598	-		-		-		-		-	-	1.598	-

Remarks

Not Applicable

	Prior Years	FY 2013		FY 2014		FY 2015 Base		FY 2015 OCO		FY 2015 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	137.103	7.547		5.110		7.201		-		7.201	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

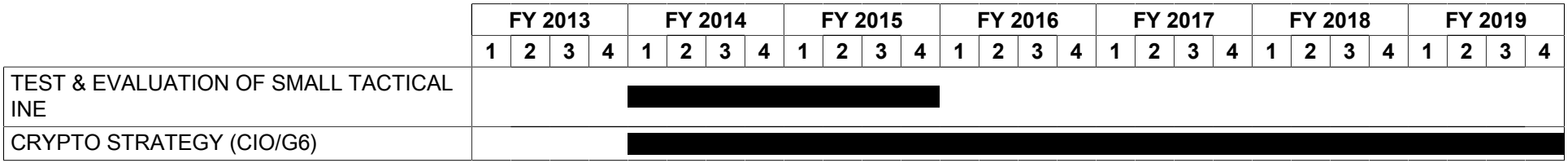

Exhibit R-4A, RDT&E Schedule Details: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 491 / *Information Assurance Development*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
TEST & EVALUATION OF SMALL TACTICAL INE	1	2014	4	2015
CRYPTO STRATEGY (CIO/G6)	1	2014	4	2019

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 501 / *Army Key Mgt System*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
501: *Army Key Mgt System*	-	6.767	1.305	1.184	-	1.184	2.303	2.154	2.466	-	-	16.179
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

A. Mission Description and Budget Item Justification

The Army Key Management System (AKMS) is the Army's implementation of the National Security Agency's (NSA) Electronic Key Management System (EKMS) program automating the functions of Communications Security (COMSEC) key management, control, and distribution, thereby limiting adversarial access to, and reducing the vulnerability of, Army Command, Control, Communications, Computers, Intelligence (C4I) systems.
NSA's legacy EKMS infrastructure began its transition to the Key Management Infrastructure (KMI) in FY2012. The transition is set to be completed by the EKMS sunset date of December 2017 and will require a minimum of 528 Management Client Nodes (MGCs) to transition the existing Army COMSEC accounts from Local COMSEC Management System (LCMS) to KMI.

AKMS supports the Mission Planning/Mission Support System (MP/MSS), a critical component of the transition to the Army Key Management Infrastructure (AKMI). MP/MSS creates a secure, highly automated interface enabling transparent provisioning of KMI products. MP/MSS is developed by NSA. Each service is responsible for integration efforts specific to their infrastructure requirements. Updates to the MP/MSS Interface Specification and additional capabilities for the base interface will be completed in FY2014.

The KOV 21 card, previously in production through NSA for use in the Simple Key Loader (SKL) and the Secure DTD 2000 System (SDS), is nearing the end of life due to unavailability of parts. Redesigning and developmental efforts using modern and readily available components for use in the Army's SKL devices are currently underway. The redesign of the current KOV 21 card has been dubbed the KOV 21-A and is an extension of the KOV 21 card as a technology insertion.

AKMS also supports the efforts of Over the Network Keying (OTNK) and Over the Air Rekeying (OTAR) for legacy devices including the Simple Key Loader (SKL). OTNK is a requirement in the Next Generation Load Device (NGLD) CPD and KMI CI-2 CPD. OTNK will allow KMI to extend Distribution Services to Type 1 devices over the network thus simplifying key change-over and task reorganization. OTAR is the method of updating and changing encryption keys in a two-way radio system over the radio channel. The use of OTAR drastically reduces the distribution of physical keying material and the physical process of loading cryptographic devices with key tapes. OTNK and OTAR developments are expected to begin in FY2016 and continue throughout the POM. Developing this capability in the SKL will allow the ~1.5M legacy End Crypto Units (ECUs) to be recognized on the KMI network until they can be upgraded to be KMI aware.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Mission Planning Mission Support System (MP/MSS) Interface	6.767	1.305	1.184
Articles:	-	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Description: The Mission Planning/Mission Support System (MP/MSS) creates a secure, highly automated interface to enable transparent provisioning of Key Management Infrastructure (KMI) products. The MP/MSS system is to be used by both the KMI system developer and MP/MSS developers to have a standard interface to electronically exchange information, enabling Warfighter Operations, achieving integration between provisioning. ***FY 2013 Accomplishments:*** Additional Mission Planning Mission Support System (MP/MSS) base capabilities were initiated during FY 13 to include 1) the addition of missing mission planning data fields based on the Communications-Electronics Research, Development and Engineering Center (CERDEC) evaluation of Sprint 9/Release 1, 2) the Release 1 backlog, along with other core software requirements related to security, and 3) the addition of access controls based on current login procedures (via medium assurance PKI, Login/Password, and KMI certificate). ***FY 2014 Plans:*** The final installment of the base capabilities for the Mission Planning/ Mission Support System (MP/MSS) will be conducted. The final result of this initiative will complete 1) the addition of missing mission planning data fields based on the CERDEC evaluation of Sprint 9/Release 1, 2) the Release 1 backlog along with other core software requirements related to security, and 3) the addition of access controls based on current login procedures via PLI, Login/Password, and KMI certificates. Additional MP/MSS capabilities will be developed in the Army Key Management Infrastructure (AKMI) program. ***FY 2015 Plans:*** Development of Army-Specific software MP/MSS API will begin in FY 15 and be carried out through FY 16. These installments of the MP/MSS effort are a continuing effort to the base capabilities developed in the Army Key Management System (AKMS) program and will ensure maximum use of KMI architecture by Army's legacy ECUs. This effort will commence after KMI MP/MSS software code is completed and delivered to the Army.			
Accomplishments/Planned Programs Subtotals	6.767	1.305	1.184

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• BA1201: *TSEC - AKMS*	24.502	13.890	10.382	-	10.382	10.719	11.142	11.298	12.640	Continuing	Continuing
• B96004: *Key Management Infrastructure*	-	3.377	41.113	-	41.113	16.853	33.328	40.418	75.171	Continuing	Continuing
• DV4: *Key Management Infrastructure*	-	1.501	2.164	-	2.164	2.364	2.169	2.072	3.333	Continuing	Continuing

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost

Remarks

Line Item & Title:
BA1201: TSEC-AKMS (OPA2)
B96004: Key Management Infrastructure (OPA2)
DV4: Key Management Infrastructure (RDTE)

D. Acquisition Strategy

Army Key Management System (AKMS) Milestone III was conducted/ approved in FY 1999. Local COMSEC Management System (LCMS) completed fielding of software v5.1.0.5 in FY 2013 and is anticipating software v5.2EE fielding to begin in FY 2014 to all Communications Security (COMSEC) custodians in order to provide encrypted key capabilities. LCMS hardware refresh began 2QFY10. AKMS supports the transition from NSA's EKMS infrastructure to the Key Management Infrastructure (KMI).

The AKMS acquisition strategy to procure Simple Key Loaders (SKLs) was updated in an Acquisition Decision Memorandum (ADM) approved by the PEO C3T Milestone Decision Authority (MDA) 3QFY02. Science Applications International Corporation (SAIC) began SKL Post Deployment Software Support (PDSS) efforts in 1QFY09. Software upgrades are released annually. SKL is currently operating on version 8.0 with version 9.0 expected in late FY 2014. In FY 2013, an Engineering Change Proposal (ECP) was initiated to address hardware obsolescence issues that impact operational mission.

The Automated Communications Engineering Software (ACES) is currently undergoing a hardware refresh to be completed in FY 2014. ACES is currently operating on version 3.3. Continued enhancements and support of AKMS next generation software tools to meet emerging Army systems' requirements are also underway.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) 501 / *Army Key Mgt System*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	0.000	2.250		0.600		-		-		-	Continuing	Continuing	Continuing
MP/MSS	C/TBD	TBD : TBD	0.000	-		-		1.184		-		1.184	Continuing	Continuing	Continuing
		Subtotal	0.000	2.250		0.600		1.184		-		1.184	-	-	-

Support ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	0.000	2.186		0.353		-		-		-	Continuing	Continuing	-
		Subtotal	0.000	2.186		0.353		-		-		-	-	-	-

Test and Evaluation ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
MP/MSS	MIPR	NSA : Linthicum, MD	0.000	2.331		0.352		-		-		-	Continuing	Continuing	-
		Subtotal	0.000	2.331		0.352		-		-		-	-	-	-

	Prior Years	FY 2013		FY 2014		FY 2015 Base		FY 2015 OCO		FY 2015 Total	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	6.767		1.305		1.184		-		1.184	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

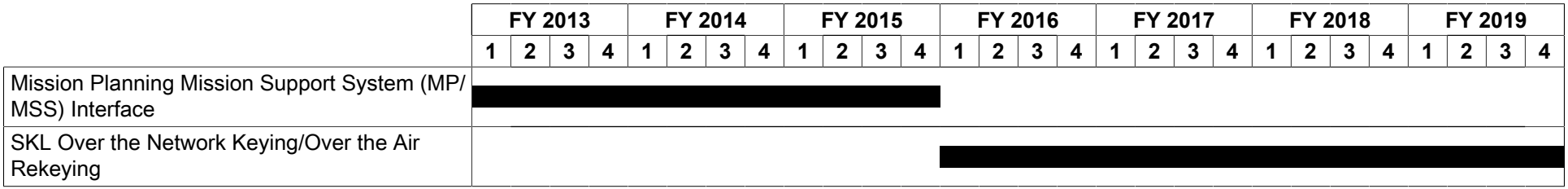

Exhibit R-4A, RDT&E Schedule Details: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** 501 / *Army Key Mgt System*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
Mission Planning Mission Support System (MP/MSS) Interface	1	2013	4	2015
SKL Over the Network Keying/Over the Air Rekeying	1	2016	4	2019

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army												Date: March 2014
Appropriation/Budget Activity 2040 / 7					R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*				Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*			
COST ($ in Millions)	**Prior Years**	**FY 2013**	**FY 2014**	**FY 2015 Base**	**FY 2015 OCO #**	**FY 2015 Total**	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Cost To Complete**	**Total Cost**
DV4: *Key Management Infrastructure (KMI)*	-	-	1.501	2.164	-	2.164	2.364	2.169	2.072	3.333	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

Note

Key management Infrastructure (KMI) (DV4) was realigned from project 491 in FY2014. KMI supports infrastructure requirements in support of Key Management.

A. Mission Description and Budget Item Justification

Key Management Infrastructure (KMI) provides an integrated, operational environment that brings essential key management personnel and functions in-band. KMI achieves an over the network keying (OTNK) solution to support emerging cryptographically modernized systems. The Army Key Management Infrastructure (AKMI) is the Army's subset of the National Security Agency's (NSA's) KMI Program supporting Department of Defense (DoD) Global Information Grid (GIG) Net Centric and Crypto Modernization Initiatives and supports emerging requirements transitioned from the Army Key Management System (AKMS).

The Mission Planning/Mission Support System (MP/MSS) for KMI creates a secure and highly automated interface to enable transparent provisioning of KMI products. The interface facilitates transparent communications between MP/MSS and KMI to achieve integration by bridging the gap between provisioning services and the communications net plan of the WarFighter. The MP/MSS Interface Specification defines the interface between the KMI Management Client Node (MGC) and the Mission Planning System operating on the Secure Internet Protocol Router Network (SIPRNET). This interface definition covers the key ordering, management, and distribution transactions that were decomposed based upon an Army Mission Planning System collaborating with KMI to fulfill mission requirements in a highly automated manner. The initial developmental efforts for MP/MSS were carried in the AKMS line through FY 2014. Continuing support relative to KMI requirements and additional capabilities for the interface are scheduled to begin in FY2015. Activities include Application Programming Interface (API) requirements that are defined in the MGC Spiral II. Major capabilities include development of mission planning data fields, access control, signature validation, Tier 3 Accounting Data Exchange, MP/MSS registration with KMI, and product request management. These interfaces are required for integration into the Army's existing Key Management Planner, Automated Communications Engineering Software/Joint-Automated Communications Electronics Operating Instruction Systems (ACES/JACS).

AKMI also supports efforts of OTNK and Over the Air Rekeying (OTAR) for emerging devices including the Simple Key Loader (SKL). OTNK is the KMI interface for providing net-centric services to the customers of KMI. OTNK is expected to allow KMI to extend Distribution Services to Type 1 devices. OTAR is the method of updating or changing encryption keys in a two-way radio system over the radio channel. The use of OTAR drastically reduces the distribution of physical keying material and the physical process of loading cryptographic devices with key tapes. OTNK and OTAR developments are expected to begin in FY2016 and continue throughout the POM.

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

The KOV 21 card, previously in production through NSA for use in the Simple Key Loader (SKL) and the Secure DTD 2000 System (SDS), is nearing the end of life due to unavailability of parts. Redesigning and developmental efforts using modern and readily available components for use in the Army's SKL and NGLD devices are currently underway. The redesign of the current KOV 21 card has been dubbed the KOV 21-A and is an extension of the KOV 21 card as a technology insertion. The KOV 21-A will also address requirements codified in the NGLD CPD and the KMI CPD that were technologically unachievable with the KOV 21 card. Through insertion of the KOV-21A into a technologically enhanced SKL, NGLD Medium requirements and OTNK can be achieved to take full advantage of the KMI architecture.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: KOV-21-A Development	-	-	2.164
Description: The KOV 21 card, previously in production through NSA for use in the Simple Key Loader (SKL) and the Secure DTD 2000 System (SDS), is nearing the end of life due to unavailability of parts. Redesigning and developmental efforts using modern and readily available components for use in the Army's SKL and NGLD devices are currently underway. The redesign of the current KOV 21 card has been dubbed the KOV 21-A and is an extension of the KOV 21 card as a technology insertion. The KOV 21-A will also address requirements codified in the NGLD CPD and the KMI CPD that were technologically unachievable with the KOV 21 card. ***FY 2015 Plans:*** Development of technology refresh to the existing KOV 21 card for use in NGLD.			
Title: Key Management Infrastructure (KMI) Awareness	-	1.501	-
Articles:	-	-	-
Description: Key Management Infrastructure Awareness initiative creates a secure, highly automated interface in providing future Over the Network Keying (OTNK) capability to legacy End Crypto Units (ECUs). This initiative will allow ECUs to receive, authenticate, and decrypt OTNK messages and increases WarFighter survivability by minimizing the need for Soldiers to travel to obtain keys. ***FY 2014 Plans:*** Additional Mission Planning/ Mission Support System (MP/MSS) capabilities projected to be developed include 1) registration of MP/MSS identities, 2) validations required for digital signature based on Key Management Infrastructure (KMI) and other medium assurance Public Key Infrastructure (PKI), 3) allowing the exchange of an electronic equivalent of a signed SF-153 (Hand Receipt, Destruction, Inventory, etc) and 4) integrating MP/MSS Application Program Interface (API) into the Army Mission Planner - Joint Tactical Network Environment NetOps Toolkit (JTNT).			
Accomplishments/Planned Programs Subtotals	-	1.501	2.164

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*	

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• B96004: *Key Management Infrastructure*	-	3.377	41.113	-	41.113	16.853	33.328	40.418	75.171	Continuing	Continuing
• BA1201: *TSEC - Army Key Mgt Sys (AKMS)*	24.502	13.890	10.382	-	10.382	10.719	11.142	11.298	12.640	Continuing	Continuing
• 501: *Army Key Management System (AKMS)*	6.767	1.305	1.184	-	1.184	2.303	2.154	2.466	-	-	16.179

Remarks

Line Item & Title:
B96004: Key Management Infrastructure (OPA2)
BA1201: TSEC-AKMS (OPA2)
501: Army Key Management System (RDTE)

D. Acquisition Strategy

Army Key Management Infrastructure (AKMI) is the Army's implementation of the National Security Agency's (NSAs) Key Management Infrastructure (KMI) ACAT ID program. The initial Army Acquisition Program Baseline (APB) for its implementation of KMI was signed on 26 Jan 2012. KMI Clients purchased in FY2012 were Low Rate Initial Production (LRIP) Management Clients (MGCs). Deliveries of LRIPS began in FY 2013. KMI MGCs purchased in FY2013 were Full Rate Production (FRP) MGCs with deliveries beginning 12 months after FRP contract award which occurred in 4QFY13. RDTE efforts are underway to provide communication within the KMI architecture for legacy devices. Current sunset for Electronic Key Management System (EKMS) is scheduled for December 2017. The Next Generation Load Device (NGLD) Capability Production Document (CPD) was signed 03 September 2013 and anticipated procurements of NGLD Small and NGLD Medium devices were slated to begin in FY14 but are delayed due to the Bipartisan Budget Act decrements. Modifications to the existing Automated Communications Engineering Software (ACES) will be made to support planning requirements and key distribution for KMI.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV4 / *Key Management Infrastructure (KMI)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
KOV-21-A	MIPR	TBD : TBD	0.000	-		-		2.164		-		2.164	Continuing	Continuing	Continuing
KMI Awareness	C/TBD	TBD : TBD	0.000	-		1.501		-		-		-	Continuing	Continuing	Continuing
		Subtotal	0.000	-		1.501		2.164		-		2.164	-	-	-

	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	-		1.501		2.164		-		2.164	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

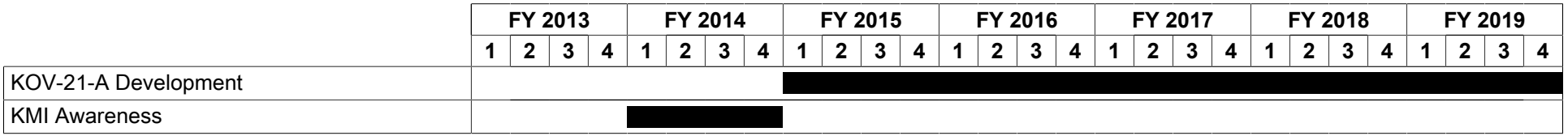

Exhibit R-4A, RDT&E Schedule Details: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV4 / *Key Management Infrastructure (KMI)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
KOV-21-A Development	1	2015	4	2019
KMI Awareness	1	2014	4	2014

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

COST ($ in Millions)	Prior Years	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO #	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
DV5: *Crypto Modernization (Crypto Mod)*	-	-	1.435	3.626	-	3.626	4.768	5.083	5.478	6.915	Continuing	Continuing
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

The FY 2015 OCO Request will be submitted at a later date.

Note

DV5 - The Crypto Modernization line was established in Sept 2012.

A. Mission Description and Budget Item Justification

This program supports the implementation of the National Security Agency (NSA) developed Communications Security (COMSEC) technologies into the Army by providing COMSEC system capabilities through encryption, trusted software or standard operating procedures, and integrating these mechanisms into specified systems in support of securing the National Network Enterprise in as transparent a manner as possible.

This entails architecture studies, system integration and testing, installation kits, and certification and accreditation of Automation Information Systems. The program assesses, develops and integrates emerging Information Assurance (IA)/COMSEC tools (hardware and software) which provide protection for fixed infrastructure post, camp and station networks as well as efforts on tactical networks. The cited work is consistent with Strategic Planning Guidance and the Army Modernization and Strategy Plan.

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
Title: Crypto Solutions for Low Bandwidth Communications at the Tactical Edge	-	0.520	-
Articles:	-	-	-
Description: This program creates tools that can be used with current and future methodologies in order to determine what amount of cryptographic solutions can be deployed at the tactical edge. This experimentation will allow for the WarFighter to have optimized solutions tailored for their specific program requirements while also showing trade-offs between competing solutions. Examples of common analysis to be performed are comparisons in encryption implementations, network initialization overhead, comparison of emerging Commercial Solutions for Classified architectures with COMSEC architectures, development of new network security and management protocols optimized for low-bandwidth environments and impact of emerging dynamic capabilities that evade or obstruct the adversary.			
FY 2014 Plans: Develop software for use in NS-2 and/or OPNet environments to target specific comparisons in COMSEC diversity and also comparisons with Commercial Solutions for Classified architectures. Study existing network security and management protocols			

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

B. Accomplishments/Planned Programs ($ in Millions, Article Quantities in Each)	FY 2013	FY 2014	FY 2015
to identify areas of improvement and propose optimizations and new protocol designs. Identify optimal placement of network discovery servers and key management infrastructure. Investigate use of single packet authorization and propose improvements that make networks and hosts less detectable			
Title: VINSON/ANDVT (Advanced Narrowband Digital Voice Terminal) Cryptograph Modernization (VACM) program ***Articles:*** ***Description:*** This program researches, assesses, tests, plans and works to integrate VACM products for the Army. The VACM program is a NSA mandated program established to replace legacy external cryptographic devices such as the KY-57, KY-99A, KY-58, KY-100 and CV- 3591 /KYV-5. In order to ensure the confidentiality, integrity and availability of classified communications, the cryptographic modules must be tested for interoperability and form fit to ensure a successful fielding. Each software release will require testing to insure comparability and interoperability. ***FY 2014 Plans:*** The program tests and evaluates developmental VACM devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. ***FY 2015 Plans:*** The program will test and evaluate Low Rate Initial Production (LRIP) of VACM devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures.	- -	0.915 -	0.500 -
Title: Cryptographic Systems Test and Evaluation ***Description:*** This program supports the Army Cryptographic Modernization Transformational Initiative. This is accomplished by providing test and evaluation capabilities to the COMSEC community in order to assess emerging technologies before being released and approved for Army use; testing can be performed on hardware, software, or network systems. ***FY 2015 Plans:*** The program tests and evaluates COMSEC devices to confirm capability and interoperability on Army networks and tactical systems as well as identifying risk areas for compliance with COMSEC regulations and procedures. The program will test and evaluate Crypto Systems compliant devices, Suite B IPSec devices built on commercial standards, Cryptographic High Value Product (CHVP), Commercial Solutions for Classified (CSfC) Standards, and new software releases to HAIPE 4.X devices in accordance with AR 700-142 Rapid Action Revision dated October 16, 2008. Tests interfaces and provides ways to insert Data At Rest (DAR) and Data In Transit (DIT) technology within the existing and future network infrastructure. Evaluates performance of technologies and provide direction on were technology will converge to insure the lowest impact on performance while providing the greatest protection from loss of sensitive data.	-	-	3.126
Accomplishments/Planned Programs Subtotals	-	1.435	3.626

Exhibit R-2A, RDT&E Project Justification: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

C. Other Program Funding Summary ($ in Millions)

Line Item	FY 2013	FY 2014	FY 2015 Base	FY 2015 OCO	FY 2015 Total	FY 2016	FY 2017	FY 2018	FY 2019	Cost To Complete	Total Cost
• 491: *Information Assurance Development*	-	5.110	7.201	-	7.201	9.619	9.912	10.795	8.809	Continuing	Continuing
• TA0600: *Information System Security Program - ISSP*	37.139	13.245	2.113	-	2.113	0.204	0.111	-	0.003	Continuing	Continuing
• B96002: *Cryptographic Systems (Crypto Sys)*	-	4.334	18.151	-	18.151	19.567	21.616	20.476	20.576	Continuing	Continuing
• BS9716: *NON PEO-SPARES*	-	2.093	3.521	-	3.521	2.551	2.597	2.680	3.225	Continuing	Continuing

Remarks

491 - Information Assurance Developement - RDTE funds - funding executed by PM and CIO/G6
TA0600 - Information System Security Program - OPA2 funds
B96002 - Cryptographic Systems - OPA2 funds
BS9716 - NON PEO-SPARES - OPA4 funds

D. Acquisition Strategy

The objective of this program is to integrate and validate hardware and software solutions to provide COMSEC superiority in order to protect against threats, increase battlefield survivability/lethality, and enable critical Mission Command activities. The objective of the Cryptographic Systems program is to provide adaptive, flexible, and programmable cryptographic systems using best practices, lessons learned and programmatic management to meet the challenge of modernizing the Army's aging cryptographic systems. The effort will support the network operations from end-to-end throughout the force and the Common Operating Environment (COE) thus mitigating Information Assurance (IA) networked vulnerabilities to National information security systems.

E. Performance Metrics

N/A

Exhibit R-3, RDT&E Project Cost Analysis: PB 2015 Army			Date: March 2014
Appropriation/Budget Activity 2040 / 7	R-1 Program Element (Number/Name) PE 0303140A / *Information Systems Security Program*	Project (Number/Name) DV5 / *Crypto Modernization (Crypto Mod)*	

Product Development ($ in Millions)

Cost Category Item	Contract Method & Type	Performing Activity & Location	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
System Engineering	C/CPIF	CECOM RDEC : APG, MD	0.000	-		0.388		0.934		-		0.934	Continuing	Continuing	Continuing
Engineering Support	C/CPFF	CACI : Aberdeen Maryland	0.000	-		0.359		1.716		-		1.716	Continuing	Continuing	-
Engineering Support	C/CPFF	Booz Allen Hamilton (BAH) : APG, MD	0.000	-		0.215		0.235		-		0.235	-	0.450	-
Engineering Support	C/CPFF	AASKI : Edgewood, Maryland	0.000	-		0.358		0.613		-		0.613	-	0.971	-
Information Assurance System Engineering Support	C/FFP	DSCI : Aberdeen, Maryland	0.000	-		0.115		0.128		-		0.128	-	0.243	-
		Subtotal	0.000	-		1.435		3.626		-		3.626	-	-	-

	Prior Years	FY 2013 Cost	FY 2013 Award Date	FY 2014 Cost	FY 2014 Award Date	FY 2015 Base Cost	FY 2015 Base Award Date	FY 2015 OCO Cost	FY 2015 OCO Award Date	FY 2015 Total Cost	Cost To Complete	Total Cost	Target Value of Contract
Project Cost Totals	0.000	-		1.435		3.626		-		3.626	-	-	-

Remarks

Exhibit R-4, RDT&E Schedule Profile: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

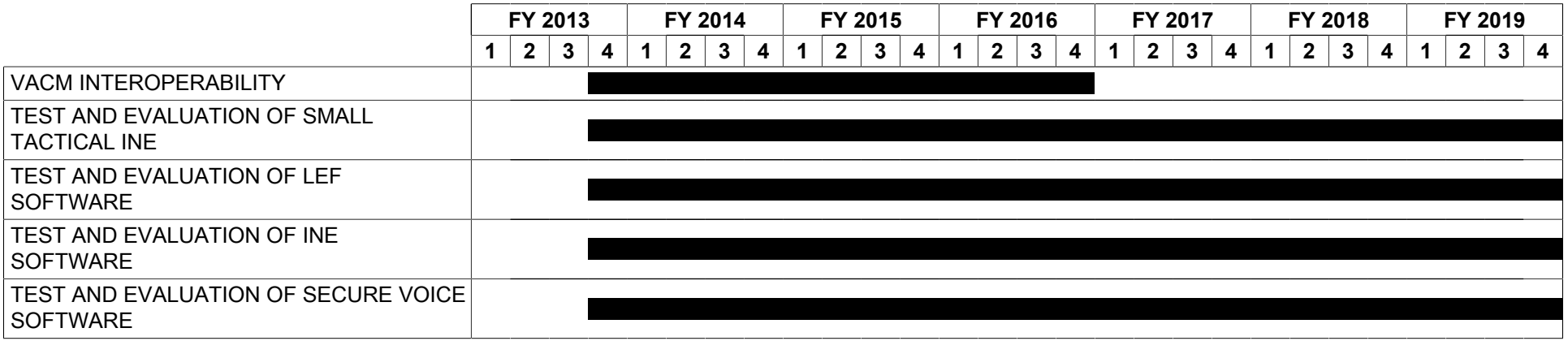

Exhibit R-4A, RDT&E Schedule Details: PB 2015 Army		Date: March 2014
Appropriation/Budget Activity 2040 / 7	**R-1 Program Element (Number/Name)** PE 0303140A / *Information Systems Security Program*	**Project (Number/Name)** DV5 / *Crypto Modernization (Crypto Mod)*

Schedule Details

	Start		End	
Events	**Quarter**	**Year**	**Quarter**	**Year**
VACM INTEROPERABILITY	4	2013	4	2016
TEST AND EVALUATION OF SMALL TACTICAL INE	4	2013	4	2019
TEST AND EVALUATION OF LEF SOFTWARE	4	2013	4	2019
TEST AND EVALUATION OF INE SOFTWARE	4	2013	4	2019
TEST AND EVALUATION OF SECURE VOICE SOFTWARE	4	2013	4	2019